Remarks

Reconsideration is requested in view of the preceding amendments and the following remarks. Claims 1-5, 12-15, and 19-21 are cancelled without prejudice, and new claim 22 is submitted for consideration. Support for new claim 22 can be found in the specification at, for example, page 14 and Fig. 1.

Rejections under 35 U.S.C. § 103(a)

Claims 1-5, 12-15, and 19-21 stand rejected as obvious from a combination of Monier, U.S. Patent 5,745,398 ("Monier") and Glaser, U.S. Patent 6,397,241 ("Glaser"). The rejection of claims 1-5, 12-15, and 19-21 is moot in view of the cancellation of these claims without prejudice.

Rejections under 35 U.S.C. § 102(b)

Claims 6-7 and 16-18 stand rejected as allegedly anticipated by Monier. Applicants respectfully traverse.

Amended claim 6 recites a cryptographic processor, comprising:

> inputs for receiving a first and a second cryptographic parameter represented as elements of a finite field; and
>
> a multiplication module configured to receive the cryptographic parameters from the inputs, the multiplication module including a first processing unit and a second processing unit configured to determine a Montgomery product of the cryptographic parameters, the first processing unit and the second processing unit configured to receive a first bit and a second bit corresponding to the first parameter, respectively, and partial words of the second parameter.

Monier does not teach or suggest such a cryptographic processor. According the Office action, Monier's Fig. 1 shows a cryptographic processor that include inputs for first and second cryptographic parameters (Monier's A and B), and multiplication circuits 19, 20 that receive a bit

of the first parameter and partial words of the second parameter. Applicants respectfully disagree. While Monier's multiplication circuit 19 is capable of receiving a bit of the parameter B and a word of the parameter A, Monier's multiplication circuit 20 is not coupled to receive a bit of the parameter B or a word of the parameter A. Instead, Monier's multiplication circuit 20 is coupled to multiply a least significant word $X_O(i)$ of $X(i) = S(i-1) + B*A_{i-1}$ and J_O. See Monier, col. 2, lines 13-15, col. 1, line 58, and Fig. 1. Thus, Monier's multiplication circuits 19, 20 are not coupled as recited in claim 6, and claim 6 and dependent claims 7-11 and 22 are properly allowable over Monier.

Amended claim 16 recites a method that comprises:

representing the first cryptographic parameter as a series of bits;
representing the second cryptographic parameter and a modulus as a series of words;
processing a first bit of the first parameter with each word of the modulus and each word of the second parameter to produce a first series of intermediate values and a contribution to the Montgomery product based on the first bit;
processing a second bit of the first parameter with each word of the modulus and each word of the second parameter, and a corresponding intermediate value from the first series of intermediate values to produce a second series of intermediate values and a contribution to the Montgomery product based on the second bit; and
combining the first contribution and the second contribution.

Monier does not teach or suggest such a method. For example, Monier does not teach or suggest producing a first series of intermediate values based on the first bit of the first parameter and words of the modulus and the second parameter, and processing the second bit of the first parameter and words of the modulus and the second parameter based on the first series of intermediate values. For at least this reason, claim 16 and dependent claims 17-18 are properly allowable.

Rejections under 35 U.S.C. § 103(a)

Claims 8-11 stand rejected as obvious from a combination of Monier, Glaser and/or the background of the present application. Applicants respectfully traverse. Claims 8-11 depend from allowable claim 6, and are allowable for at least this reason.

Conclusion

In view of the preceding amendments and remarks, all pending claims are in condition for allowance and action to such end is requested. If any issues remain, particularly concerning the Monier reference, Applicants respectfully request a telephonic interview to be conducted at the Examiner's convenience.

Respectfully submitted,

KLARQUIST SPARKMAN, LLP

By 

Michael D. Jones
Registration No. 41,879

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 595-5300
Facsimile: (503) 228-9446